ГУО «Белорусский государственный университет  
информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №4

по дисциплине

«Тестирование веб-ориентированных приложений»

«Автоматизация тестирования безопасности интернет-ориентированного приложения.»

Выполнил:

Сенько Н.В.

Гр. 551002

Проверил:

Шостак Е.В.

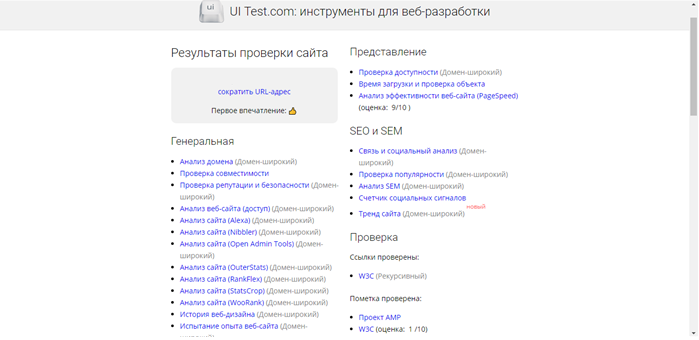
Минск, 2018 г

Задание: самостоятельно выбрать и установить любое свободно распространяемое веб-ориентированное программное обеспечение, выбрать и установить средство автоматизированного тестирования безопасности, провести исследование и задокументировать обнаруженные дефекты.

Для развертывания сервера с интернет-магазином было выбрано свободное программное обеспечение работы интернет-магазина bizhustil. Развертывание проводилось с помощью средства Wordpress. Необходимым является наличие PHP, Apache и MySQL.

В качестве средства автоматизированного тестирования безопасности было выбрано програмное средство UI Test.com: инструменты для веб-разработки.  
Это сканер, который делает различные запросы к вашему серверу и выявляет различного рода уязвимости в безопасности, такие как: незащищенное соединение, XSS и CLRF-атаки, SQL-инъекции, подбор пароля брутфорсом и еще множество других потенциальных уязвимостей веб-приложения.

Результаты тестирования таковы:



Сразу хочется обратить внимание на довольно большое время отклика, если учесть, что сервер локальный. За всю проверку ПС обнаружило потенциальные уязвимости.

Интернет-магазин не подвержен CSRF-уязвимости. На сайте найдены формы, в которых реализована защита от CSRF-атак.

Интернет-магазин использует защищенное HTTP-соединение, что не позволяет злоумышленникам вторгаться в обмен данными между сервером и клиентом и тем самым перехватывать потенциально важную информацию.

Еще одним дефектом является отсутствие максимально допустимого количества попыток ввода пароля, тем самым сайт подвержен атаке брутфорсом, т.е. злоумышленник может просто подбирать пароли и отправлять неограниченное число запросов на сервер с попыткой входа.

Других уязвимостей выявлено не было, таким образом безопасность сервера находится на довольно высоком уровне и исправление выше описанных уязвимостей позволит защититься от наиболее распространенных атак на сервер.